Public Wireless

A wireless-enabled laptop can make you more productive outside the office, but it can also expose you to a number of security threats. Here are some of the security threats and safety tips to keep in mind when using public wireless.

Wireless Threats

Evil Twin Attacks

Criminals sometimes set up a rogue wireless access point near a legitimate public wireless hot spot. Unsuspecting users will connect to the criminal's bogus signal. Because the victim is connecting to the internet through the criminal's system, it's easy for the criminal to use specialized tools to read any information the victim sends over the internet.

Wireless Sniffing

Many public wireless hot spots are not secure, and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted "in the clear," malicious users can use "sniffing" tools to obtain sensitive information such as passwords, social security numbers, and bank account/credit card numbers.

Peer-to-Peer Connections

Many laptop computers, particularly those equipped with 802.11-type WiFi wireless networking cards, can create ad hoc networks if they are within range of one another. These networks enable computer-to-computer connections. An attacker with a network card configured for ad hoc mode and using the same settings as your computer may gain unauthorized access to your sensitive files. Many PCs ship from the manufacturer with wireless cards set to ad hoc mode by default.

Shoulder Surfing

In public wireless areas, the bad guys don't even need a computer to steal your sensitive information. The fact that you may be conducting state business in a public space is opportunity enough for them. If close enough, they can simply glance over your shoulder as you type. By simply watching you, they can steal all kinds of sensitive, personal information.

Safety Tips While Using Wireless

Watch What You Do Online

Public wireless tends to be unsecure and unencrypted so be careful about what you do online. Another user could be monitoring your activity. Avoid the following when using public wireless to go online:

- online banking,
- working with confidential information, and
- typing passwords or credit card numbers .

Disable File Sharing

File sharing in public wireless spaces can be dangerous. To prevent attackers from gaining access to your sensitive files, you should disable file sharing when connecting to a public wireless hot spot. Consult your agency's IT staff to learn how to disable file sharing.

Be Aware of Your Surroundings

When using a public wireless hot spot, you should be aware of what's going on around you. Can others view your screen? Are you sitting near a window through which someone, using binoculars, could get a view of your screen? Consider whether it is essential to connect to the internet. If an internet connection is not needed, disable wireless networking altogether.

Piggybacking

Finally remember that using someone else's wireless internet connection without permission (piggybacking) to conduct state business is not allowed.

Source: US-CERT and Iowa Department of Administrative Services - Information Security Office,